

УДК 004.77

Семерюк Т.М.¹, Неласа Г.В.²

¹ асп. НУ «Запорізька політехніка»

² канд. техн. наук, проф. НУ «Запорізька політехніка»

УПРАВЛІННЯ РИЗИК-ОБ'ЄКТАМИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Темпи розвитку сфери інформаційних технологій зумовлюють необхідність прояву пильної уваги до питань забезпечення інформаційної безпеки, а також відповідності її стану швидких змін в технологіях, зменшення вірогідності реалізації ризиків, пов'язаних з інформаційними загрозами. Метою управління ризиками інформаційної безпеки є підтримування їх на прийнятному для організації рівні. Для вирішення поставленої задачі створюються комплексні системи інформаційної безпеки. При створенні таких систем постає питання вибору засобів захисту, які забезпечують зниження, виявлених в процесі аналізу, ризиків інформаційної безпеки без надмірних витрат на впровадження і підтримку цих засобів. Аналіз ризиків інформаційної безпеки дозволяє визначити необхідну і достатню сукупність засобів захисту інформації, а також організаційних заходів, спрямованих на зниження ризиків інформаційної безпеки, і розробити архітектуру системи інформаційної безпеки організації, яка буде максимально ефективна для її діяльності і спрямована на зниження її ризиків інформаційної безпеки.

Ризик інформаційної безпеки є потенційна можливість використання вразливостей засобів конкретної загрози для заподіяння шкоди об'єкту.

Існує також умовна класифікація ризиків: за джерелом ризику (наприклад: хакерські атаки, фінансові помилки, вплив державних регуляторів, юридичні претензії контрагентів, негативний інформаційний вплив конкурентів); по цілі (інформаційні засоби, матеріальні ресурси, репутація); за тривалістю впливу (операційні, тактичні, стратегічні).

Методики і рекомендації базуються на двох основних підходах до подання оцінок інформаційних ризиків: якісному і кількісному. Завданням

якісної оцінки є визначення можливих видів ризиків, оцінка принципового рівня серйозності загроз, а також виділення факторів, що впливають на рівень обґрунтування різних можливих контрзаходів.

Кількісні методики надають реальні і осмислені чисельні значення всім елементам процесу аналізу ризиків. Кількісний аналіз дозволяє отримати конкретне значення ймовірності реалізації загрози. Кожен елемент в процесі аналізу вводиться в кількісному вигляді в рівняння для визначення загального і залишкового ризику. Якщо застосовуються якісні методи, можливі ризики порушення інформаційної безпеки повинні бути впорядковані за ступенем їх небезпеки з урахуванням факторів, як рівень загрози і вразливості. Ризики можуть бути оцінені за допомогою кількісних шкал. Це дасть можливість спростити аналіз існуючих загроз в інформаційних системах і вибір заходів захисту. Однак в цьому випадку пред'являються більш високі вимоги до шкал вимірювання вихідних даних. Наявність декількох загроз (вразливостей) характеризується відповідними частковими ризиками, сукупний вплив яких описується певним інтегральним ризиком, оцінювання якого в загальному випадку може бути досить складним [1]. Методики управління ризиками, розроблені за рекомендаціями стандартів, найчастіше спираються на перебірний підхід: розглядається кілька можливих варіантів побудови засобів захисту інформації, в яких рівні ризиків (інтегрального ризику) зменшуються до прийнятних значень. Перевагою якісного підходу є його простота, мінімізація термінів і трудовитрат на проведення оцінки ризиків. Перевагою кількісного підходу є точність оцінки ризиків, наочність результатів, недоліками - складність, висока трудомісткість і тривалість виконання.

Конкретні вимоги до заходів об'єктового захисту визначаються за результатами спеціальних досліджень технічних засобів з урахуванням встановленої категорії об'єкта, що захищається, в залежності від ступеня конфіденційності оброблюваної інформації і умов розміщення. Різні атаки вимагають різних технологічних рішень по забезпеченню інформаційної безпеки об'єктів атак. Оскільки кількість атак і їх модифікацій обчислюється більш, ніж п'ятизначним числом, то розробляються різні класифікації підходів забезпечення інформаційної безпеки, що охоплюють групи атак. При захисті конкретного об'єкта атаки від ризику кожна з функцій безпеки може бути модифікована. Наприклад, можна змінити алгоритм шифрування, змінити налаштування брандмауера, застосувати новий правовий акт і т.і.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1.Nazarov A.N., Nguyen Xuan Tien, Tran Minh Hai. Modeling of information attacks, and security risk assessment facilities. T-Comm. 2016.Vol. 10. No.8, pp. 69-78.